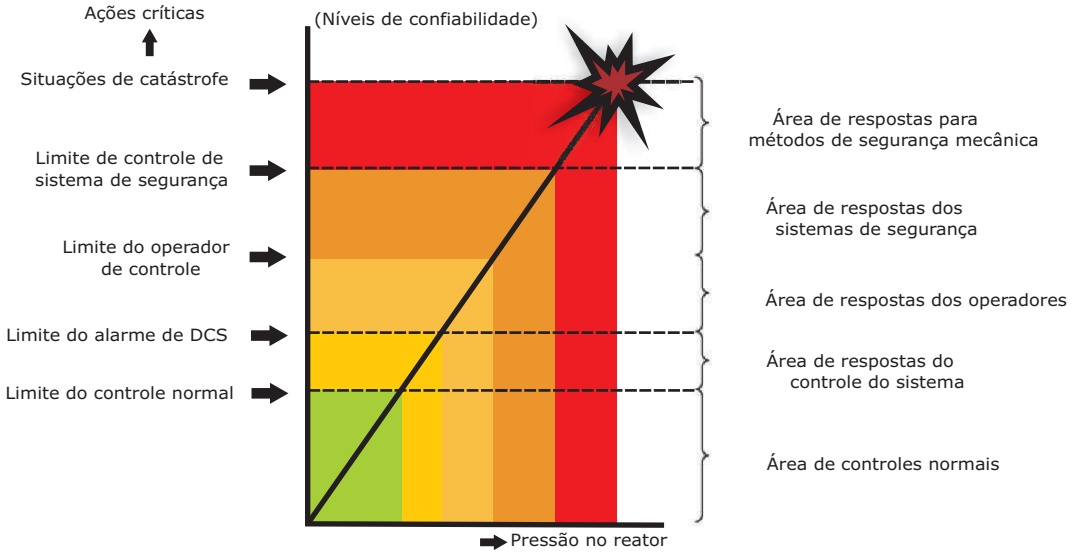

Figura 1: Diagrama de Segurança

O que é Segurança Funcional

A definição formal de segurança da ISO/IEC 61508 é "isenção de riscos inaceitáveis de lesões físicas ou danos à saúde das pessoas seja, direta ou indiretamente, como resultado da prejuízos à propriedade ou ao meio ambiente".

Segurança funcional é a parte da segurança que depende da operação correta de um sistema de segurança. Por exemplo, um instrumento de temperatura que utiliza um sensor térmico para proteção do enrolamento de um motor elétrico para desenergizá-lo antes que superaqueça, é um sistema de segurança funcional. Porém, prever no projeto um isolamento específico para suportar altas temperaturas não é um exemplo de segurança funcional (mesmo que ainda seja um caso de segurança e possa proteger contra esse risco). Tanto a segurança como a segurança funcional não podem ser determinadas sem considerar os sistemas como um todo e o meio ambiente com o qual interagem. Em geral, isto se aplica a todos as metodologias relativas a nível de segurança utilizadas para proteger as pessoas de qualquer risco.

Na instalação de um processo, este em si deve ser mantido dentro dos limites de segurança operacional por um sistema de controle. Este sistema controla o processo para prevenir a ocorrência de variações decorrentes da influência distúrbios externos. Quando o sistema de controle não consegue manter o processo dentro de seus limites, um alarme é acionado e o operador assume. O operador tem a capacidade de supervisionar todo o processo e fazer os ajustes que trarão o processo de volta ao controle automatizado normal.

Este é um método padrão para manter a segurança numa indústria de processo. Contudo, em muitos casos, isto não é suficiente para alcançar um nível de segurança aceitável. Este nível de segurança aceitável é uma questão muito crítica, pois é a base dos sistemas de segurança funcional. Se um operador falhar em trazer o processo de volta aos seus limites de segurança operacional, um sistema de segurança independente deve assumir. Veja a figura 1 acima.

Hazop

A necessidade de um sistema de segurança depende dos resultados de um estudo durante o qual os riscos significantivos são identificados. Este estudo é denominado Hazop (Hazard & Operability - Riscos & Operacionabilidade).

É importante notar que segurança funcional é apenas um método de lidar com riscos e outros meios para sua eliminação ou redução, tal como segurança inerente por intermédio do projeto, são de suma importância.

Há dois requisitos que definem o sistema de segurança: a função relacionada à segurança e à confiabilidade relacionada à segurança. O primeiro requisito é função do sistema de segurança e é derivado da análise de risco. A segunda é a probabilidade desta função ser executada adequadamente e deriva da avaliação de risco.

O eixo horizontal na figura mostra o nível de pressão. O aumento da pressão e/ou risco é diretamente proporcional à possibilidade de uma situação perigosa. O eixo vertical mostra os níveis de confiabilidade exigida ou a integridade exigida da função de segurança, denominado Nível de Integridade de Segurança ou SIL (Safety Integrity Level).

Nivel de Integridade e Classificação de Segurança

SIL é uma classificação do nível de integridade da função de segurança exigida, onde 1 é o mais baixo e 4 é o mais alto nível de integridade. Atualmente, a utilização industrial das normas IEC61508 e IEC61511 está se tornando uma necessidade para a classificação de sistemas de segurança, e tais normas especificam ações em termos de classes de SIL. É um sistema facilmente entendido que prevê, de forma relativamente simples, a determinação do nível de segurança funcional de uma instalação de processo.

Engenheiros envolvidos em projetos de sistemas de ações de emergências na indústria de processo devem estar cientes de questões relevantes, tais como as técnicas disponíveis, as exigências de diferentes normas e as exigências das autoridades envolvidas. A norma internacional IEC61511 é específica para a indústria de processo, tendo como apoio estrutural a publicação IEC61508, da IEC — International Electro-Technical Commission.

Funções de segurança são realizadas por sistemas elétricos, eletrônicos ou eletronicamente programáveis. Estes sistemas devem assegurar que, no caso de um reator sobre pressurizado, a pressão seja rapidamente trazida de volta a um nível seguro, conforme a figura 2.

A integridade desta função depende da severidade dos efeitos de uma falha. Os efeitos do perigo estão relacionados a três aspectos: pessoal, financeiro e ambiental. Estas três categorias recebem uma classificação em quatro níveis correspondentes ao SIL. Na escala de classificação de segurança, níveis mais elevados, como o SIL 2, definem os requisitos de integridade para esta função de segurança. Isto se chama classificação de segurança. No exemplo abaixo, a pressão está sendo medida, a saida está conectada ao sistema de segurança e a saída do sistema está conectada a uma válvula de segurança.

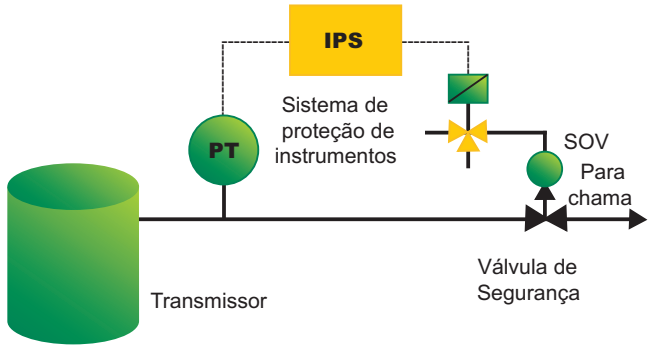

Figura 2 : Exemplo de um reator pressurizado

A integridade desta cadeia de controle depende da confiabilidade de todos os componentes e esta confiabilidade é descrita como razão de falha (FR). Em outras palavras: a FR (λ) é a probabilidade de um dispositivo não responder a uma mudança de variável de entrada sem ser detectada. Um dispositivo que falha 1 de 1000 solicitações por ano tem uma razão de falha de 0,001/ano.

Cálculo do PFD e Avaliação de Segurança

Como qualquer dispositivo perde confiabilidade sem manutenção ou testes apropriados, a razão de falha por si só não é o suficiente para especificar a integridade. Um dispositivo testado frequentemente tem integridade maior do que um que nunca foi testado e é menos suscetível a falhas. Assim é expresso o valor da PFD - Probabilidade de Falha sob Demanda. A PFD média de um dispositivo é calculada como PFD_{avg} = 0,5. FR.Ti, onde Ti é o intervalo de teste na mesma base de tempo que a FR. O SIL se relaciona à PFD da cadeia total da qual as funções de segurança dependem. Essa cadeia consiste basicamente de três componentes: o transmissor, o solucionador lógico e o elemento final. Na figura 2, estes são o transmissor, o IPS e a válvula de segurança.

A confiabilidade do transmissor depende das razões de falha da interface do processo, do sensor, do transmissor, das caixas de junção, do cabo e dos elementos de interface, tais como a barreira e o cartão de entrada de informação do solucionador lógico. A PFD do transmissor é calculada adicionando as FRs individuais, seguido pelo cálculo conforme a fórmula citada acima. O mesmo procedimento se aplica ao elemento final. Para o cálculo da média da PFD da cadeia, as PFDs dos três componentes são somados. Trata-se da avaliação da segurança da cadeia de controle.

Outra maneira de aumentar a integridade do circuito é aumentar o número de transmissores ou elementos finais - votação um-de-dois (1oo2) ou votação um-de-três (1oo3). Dispositivos múltiplos também podem ser utilizados redundantemente para executar a mesma função de segurança. Fórmulas diferentes são aplicáveis para obter a média apropriada de PFD. Na tabela a seguir encontra-se a relação entre PFD e SIL.

Nivel de Integridade de Segurança	Redução de riscos pelo sistema de segurança	Probalidade de falhas em demanda
SIL < 1	Sem requerimentos	Sem requerimentos
SIL 1	> 10	< 0,1
SIL 2	> 100	< 0,01
SIL 3	> 1.000	< 0,001
SIL 4	> 10.000	< 0,0001

Elementos Finais

O elemento final muitas vezes consiste de uma válvula solenoide, um atuador e uma válvula de processo. Válvulas solenóide são uma parte essencial da cadeia de segurança, sendo que controlam diretamente os atuadores das válvulas ON/OFF. Em uma operação normal, a válvula solenóide é energizada e abre, acionando o atuador. Quando o solucionador de lógica é acionado, a válvula é desenergizada, liberando a pressão de alimentação para o atuador, o que faz com que a válvula mude para sua posição segura. A segurança é totalmente dependente da confiabilidade da válvula piloto, ou seja, sua fabricação deve seguir os mais altos padrões de qualidade e os testes, conduzidos sob as condições mais severas. As válvulas piloto da Asco, modelos 8314, 8316, 8320, 8327 e 551, foram testadas com sucesso pelos organismos de certificação de produtos e são apropriadas para uso em aplicações de segurança até SIL 3 e SIL 4.

Estes são os níveis SIL mais elevados que podem ser alcançados. A integridade da cadeia de segurança é influenciada não somente pela válvula piloto, mas também pela válvula de processo. Como esta válvula permanece em uma posição operacional fixa a maior parte de sua vida útil, ela poderá ficar travada nesta posição. Se isto acontecer, ela não se moverá mesmo se o solenóide for acionado. Portanto, é essencial aplicar testes funcionais frequentes. No passado, muitas vezes estes testes eram executados manualmente e os deslocamentos da haste e do obturador eram observados. Válvulas para aplicações de segurança modernas podem ser equipadas com Sistemas de Controle Redundantes - RCS ASCO que possuem certificação Exida para até SIL 3, incorporando segurança e continuidade operacional ao processo.

Além de sua função de redundância, o RCS ASCO possibilita a execução do Partial Stroke Test e seu sistema de manifold com by-pass permite manutenção e teste das válvulas solenóide online, sem necessidade de parada ou interrupção do processo produtivo.

O RCS ASCO disponibiliza uma grande variedade de diagnósticos das condições operacionais das válvulas de processo. Funções e opcionais, tais como a utilização de pressostatos para sinalização remota de sistema by pass, indicação de falhas das solenóides. Disponível nos modos de operação 1oo1 (uma válvula solenóide sempre em stand-by) ou 2oo2 (duas válvulas solenóide simultaneamente energizadas), possui ainda três diferentes configurações: Normalmente Fechado, Normalmente Aberto e Dupla Ação.